ISTRUZIONI PER RESISTERE AI VIDEO-PIRATI

Dalle Deepfake all'uso dell'intelligenza artificiale, i nuovi pericoli del web. Tre contromosse

di **Umberto Torelli**

Posta elettronica, cloud computing e mondo Iot (Internet degli oggetti). Questi i tre veicoli di infezione da cui si propagheranno i maggiori attacchi informatici nei prossimi mesi. E spetta alle email il primato della vulnerabilità, perché nel 2019 sono state 50,4 miliardi quelle compromesse da virus, link malevoli e frodi arrivate su computer e smartphone. A conti fatti, visto che nel mondo sono 4,5 miliardi gli utenti Internet, significa che in media ognuno ne ha ricevute oltre dieci. Anche all'insaputa degli stessi destinatari.

La tendenza

Lo rivelano gli ultimi dati di Trend Micro, l'azienda giapponese specializzata in sicurezza informatica. Il 2020 si annuncia come anno delle deepfake, i video e gli audio falsi generati dall'intelligenza artificiale (AI). Spiega Gastone Nencini, country manager di TrendMicro per l'Italia: «Si tratta di contenuti audio e video contraffatti grazie a sofisticati software di intelligenza artificiale, dove alle persone vengono fatte dire e fare cose non avvenute nella realtà, bensì confezionate come in una fiction».

È dunque l'evoluzione delle fake news, le false notizie sul web conosciute negli ultimi anni. Con le deepfake i cybercriminali non falsificano i soli indirizzi di posta elettronica ma, approfittando degli elementi audiovisivi, rendono anche credibili i messaggi veicolati. Gli utenti sono così stimolati e incuriositi a visitare link esterni. Risultato: scaricano app infette e mettono a rischio la memoria di Pc e telefonini. Questa vulnerabilità si aggiungerà nel corso del 2020 all'arrivo di «agenti intelligenti» e nuovi programmi di phishing, caricati sulla nuvola informatica per catturare prima e aggregare poi i dati delle persone, creando cartelle digitali personali da usare nel tempo. L'obiettivo? Tracciare i profili delle identità online con le informazioni sulle nostre abitudini.

Gli archivi sul cloud

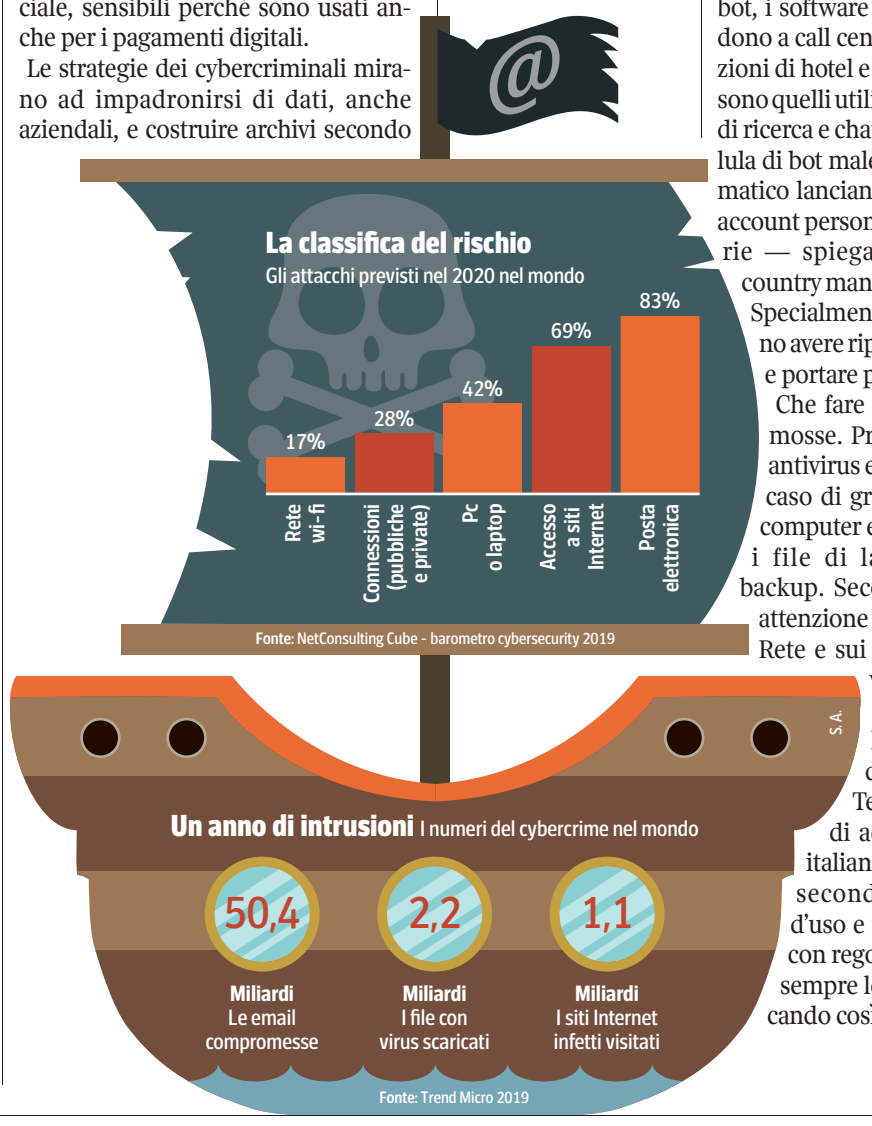
Ed è proprio «la pesca web» di dati sensibili la nuova insidia per 45 milioni di utenti del Belpaese. Tante le fonti da cui i pirati informatici attingono informazioni seminate da ignari (non sempre) utenti su Internet e social. Dalle credenziali bancarie, ai programmi fidelity, inclusi accumuli di miglia aeree e recensioni dei ristoranti. Oltre ai dati che consentono il riconoscimento facciale, sensibili perché sono usati anche per i pagamenti digitali.

Le strategie dei cybercriminali mirano ad impadronirsi di dati, anche aziendali, e costruire archivi secondo la regola del «prima o poi verranno utili» per rivenderli e commettere furti digitali. Bisogna poi prestare attenzione al fenomeno emergente degli empotet. Spiega Paolo Frizzi, ceo di Libraesva, azienda di Lecco specializzata in protezione informatica: «Sono false email generate dai malviventi servendosi di quelle vere rubate dalle caselle di posta degli utenti». Questi ultimi, visto che compare il loro nome, credono di rispondere a corrispondenze sicure in cui vengono rivelate informazioni e dati sensibili.

Attenzione anche al fenomeno dei bot, i software robotizzati che rispondono a call center, aiutano in prenotazioni di hotel e operazioni bancarie. Ci sono quelli utili e buoni legati ai motori di ricerca e chat vocali. «Ma il web pullula di bot malevoli che in modo automatico lanciano attacchi, sottraggono account personali e fanno frodi bancarie — spiega Maurizio Desiderio, country manager di F5 Networks —. Specialmente per le aziende, possono avere ripercussioni sul business e portare perdite economiche».

Che fare per proteggersi? Tre le mosse. Primo, tenere aggiornati antivirus e sistemi operativi. E nel caso di gravi attacchi formattare computer e telefonini, ricaricando i file di lavoro da precedenti backup. Secondo, prestare grande attenzione ai dati che postiamo in Rete e sui social. Quelli sensibili vanno inseriti solo in siti protetti, non certo in link ricevuti via email da indirizzi sconosciuti. Terzo, le password, chiavi di accesso ai dati. Solo un italiano su dieci le diversifica secondo app e programmi d'uso e meno del 5% le cambia con regolarità. Gli altri digitano sempre le stesse due-tre spalancando così le porte ai pirati.

@utorelli



Metropolis

Ingerisci un led e lo stent si scioglie

Si scompongono a comando, sollecitati da un particolare tipo di luce ingeribile: sono i dispositivi realizzati al Mit, che potrebbero eliminare alcune procedure endoscopiche. Molti dispositivi medici vengono impiantati per trattare, diagnosticare o monitorare i disturbi gastrointestinali. Svolto il lavoro, il più delle volte devono poi essere rimossi con chirurgia endoscopica. La nuova tecnologia si basa invece su un nuovo idrogel sensibile alla luce: ha un legame chimico che si rompe se è esposto a una lunghezza d'onda della luce dal blu all'ultravioletto. Essendo un gel, può essere facilmente modellato. È poi biocompatibile, come i prodotti della sua decomposizione. Durante la sperimentazione suina i ricercatori hanno utilizzato il materiale come sigillo per un palloncino bariatrico e per uno stent esofageo. La rimozione di entrambi è avvenuta tramite l'ingestione di un Led, che li ha degradati.

Idrogel
Il dispositivo medico inventato al Mit per trattare i disturbi gastrointestinali. Una volta ingerito, si degrada senza bisogno di essere rimosso con la chirurgia

Caccia al neutrone

Un rilevatore di neutroni che può stare in tasca: l'hanno inventato alla Northwestern University, negli Usa. Attualmente la capacità di scovare materiali nucleari è propria di rilevatori grandi a volte quanto una parete: individuano i neutroni che atomi di metalli pesanti, come uranio e plutonio, espellono dai loro nuclei, e avvisano emettendo luce. Il nuovo dispositivo, in un materiale ricco di litio, è un semiconduttore e non emette luce, ma registra i segnali elettrici indotti dai neutroni. In fretta e da fonti anche molto deboli: una frazione del materiale può assorbire la stessa quantità di neutroni di un dispositivo gigante, da qui i rilevatori tascabili. I rilevatori di neutroni sono utilizzati per la sicurezza e in radioprotezione, astronomia, scienze dei materiali, cristallografia.

Cristina Pellecchia

Pit Spot

SisalPay, il fascino di dire «Stai sereno»

a cura di **Aldo Grasso**
pitspotcorriere@gmail.com
in collaborazione con
Massimo Scaglioni

Elogio della «comfort zone»: che cosa succede quando ci sentiamo «sereni e sicuri»? La reazione fisica più evidente di uno stato di serenità e relax è quella ci porta a chiudere gli occhi, fiduciosi sul fatto che non ci sono pericoli che ci minacciano. Utilizza questa metafora corporea lo spot di lancio della Carta SisalPay, protagonista di una campagna omnicanale che sottolinea il posizionamento del prodotto, uno dei tratti essenziali trattandosi di denaro, spesa (e risparmi): la sicurezza. E la metafora funziona in maniera analogica: la sicurezza degli «occhi chiusi» è la stessa che, è il messaggio, accompagna ogni pagamento con la Carta SisalPay. Infatti, dicono le ricerche, l'atto del pagamento attraverso una carta, nei canali fisici e soprattutto online, è ancora percepito come un momento di grande attenzione da parte del consumatore, che ritiene le insidie dietro l'angolo. Da questo nasce il concept creativo «A occhi chiusi», che fa leva sul benefit chiave della nuova carta SisalPay, nata da un brand che da più di dieci anni lavora sulla semplificazione della vita degli italiani, per migliorare e rendere più sicuri i pagamenti di tutti i giorni. Lo spot — creato dall'agenzia Gitto Battaglia — racconta efficacemente una serie di «momenti di serenità»: una ragazza è distesa su un tappeto, davanti a un camino, appoggiata a un peloso cucciolone; in un teatro, alcune persone stanno testando la fiducia reciproca lasciandosi cadere fra le braccia dei compagni; in una piscina una ragazza si lascia andare nell'acqua sapendo di essere sorretta da una mano amica; una rockstar viene letteralmente sollevata dalle braccia dei fan; un ragazzo si affida alla guida sicura del padre. Tutte queste situazioni vengono messe in parallelo con l'acquisto online con SisalPay: «Fai acquisti online in totale sicurezza — conclude la voce fuori campo — e controlli la tua spesa». Il claim, centrato sul «pagare a occhi chiusi», sintetizza in modo altrettanto efficace il senso dell'intera campagna.